Informatiebeveiligingseisen aan leveranciers van Wielpassagesensoren 2026

Dit betreft een systeem van wielpassagesensoren t.b.v. het meten van bezetting van emplacementen (NCBG) van Botlek (stamlijnen), Zaanstraat en Venlo.

Leverancier levert, installeert en onderhoudt de complete, gevraagde oplossing voor het aanleveren van data uit de wielpassagesensoren.

Het projectteam Last Mile Spoor onderhoudt een dashboard waarmee de eindgebruikers (CO, CV) het gebruik van de emplacementen kunnen monitoren, sturen en optimaliseren op basis van verkregen inzichten in de (on)benutte spoorcapaciteit.

De kenmerken t.a.v. de informatiebeveiligingseisen betreffen:

- Tier2
- Technische gegevens
- Locatiegegevens
- Clouddiensten
- Communicatievoorzieningen
- Digitale toegangsbeveiliging

Architectuureisen worden nog aangeleverd.

Versiebeheer

Versie	Datum	Auteur	Wijziging / Opmerking
0.9	30-04-2026	Douwe Doevendans	Conceptversie
1.0	11-05-2026	Douwe Doevendans	Definitief na afstemming ISO

Thema	Eis
B. Awareness	De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers periodiek en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).
C. Bedrijfscontinuïteit; a)	De leverancier heeft aantoonbaar en actueel inzicht in de risico's binnen zijn bedrijfsprocessen die een bedreiging zouden kunnen vormen voor de continuïteit en/of veiligheid van de bedrijfsprocessen van ProRail.
C. Bedrijfscontinuïteit; b)	Voor het betreffende IT- of OT-asset dient ten minste volgens het ingerichte back-up proces een back-up te worden gemaakt na elke (functionele) systeemwijziging of op vooraf bepaalde, periodieke termijnen. Indien het om welke reden dan ook niet mogelijk is om een back-up te maken, dan wordt dit vastgelegd en, op basis van een risicoanalyse, een alternatieve werkwijze gekozen en beschreven.

D. Certificeringen en normenkaders	De leverancier garandeert dat hij voldoet aan alle toepasselijke verplichtingen voortvloeiend uit de komende Cyberbeveiligingswet, inclusief maar niet beperkt tot: 1. Het treffen van passende technische en organisatorische maatregelen ter beheersing van cyberbeveiligingsrisico's; 2. Het melden van betekenisvolle cyberincidenten aan de relevante toezichthoudende autoriteiten en aan de opdrachtgever binnen 24 uur na ontdekking; 3. Het uitvoeren van regelmatige risicoanalyses en het bijwerken van beveiligingsmaatregelen; 4. Het waarborgen van de beveiliging van persoonsgegevens en bedrijfsinformatie van de opdrachtgever; 5. Het faciliteren van audits en inspecties door of namens de opdrachtgever om naleving van deze clausule te verifiëren. Indien de leverancier nalaat te voldoen aan deze verplichtingen, behoudt de opdrachtgever zich het recht voor om het contract per direct te ontbinden en/of schadevergoeding te eisen.
E. Contactpersoon	Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in bijvoorbeeld de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.
G. Exit-strategie	De leverancier beschikt over een uitwerking van een exit-strategie, die goedgekeurd is door ProRail. Deze strategie omvat minimaal afspraken over hoe de data overgedragen en daarna verwijderd/vernietigd wordt bij wisseling van leverancier of overname van de dienst door ProRail.
H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.
I. Gegevensverwerking en -opslag; a)	De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
I. Gegevensverwerking en -opslag; b)	De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.
J. Geheimhouding	Ter waarborging van de vertrouwelijkheid van Vertrouwelijke en/of Geheime informatie wordt een Non Disclosure Agreement (NDA) of vergelijkbare vertrouwelijkheidsverklaring ondertekend door de leverancier (en indien relevant door ProRail). De leverancier verplicht zijn personeel aantoonbaar om de geheimhoudingsverplichting na te komen.
K. Incidenten; a)	Bij constatering van een kwetsbaarheid, beveiligingsincident of datalek dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail, bereikbaar op nummer 0882312600, en de betreffende contractmanager.
K. Incidenten; b)	De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden die veiligheid van het systeem raken direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan een toezichthouder zoals de Autoriteit Persoonsgegevens of IL&T. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
K. Incidenten; c)	De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.
L. Monitoren en loganalyse; a)	Monitoring is ingericht voor alle IT- en OT-systemen. Wanneer monitoring niet mogelijk is of niet rendabel is, dan dient hiervoor een risico gebaseerde redeneerlijn te worden opgesteld. Monitoring van de remote toegang en beheer op afstand dient altijd te worden ingericht.
L. Monitoren en loganalyse; b)	Activiteiten van gebruikers en beheerders dienen ten behoeve van audittrailing vastgelegd te worden in beveiligde registraties. Deze registratie wordt op verzoek van ProRail door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld.

M. Onderaanneming en toeleveranciers; a)	De leverancier dient inzicht te geven in welke derden mogelijk toegang kunnen hebben tot ProRail data. Denk aan hosting providers, softwareleveranciers, support partijen, subverwerkers, etc.
M. Onderaanneming en toeleveranciers; b)	Alle voorwaarden en eisen van ProRail op het gebied van informatiebeveiliging die gelden voor de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
M. Onderaanneming en toeleveranciers; c)	De leverancier moet desgevraagd inzage geven in de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden.
M. Onderaanneming en toeleveranciers; d)	Het is de leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ProRail, de uitvoering van een contract geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten. Deze toestemming zal niet op onredelijke gronden geweigerd worden.
M. Onderaanneming en toeleveranciers; e)	ProRail wordt zo snel mogelijk op de hoogte gebracht indien de leverancier wijzigingen aanbrengt bij het uitbesteden van zijn eigen (deel)processen. Hierdoor kan ProRail bepalen of er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen in de wijze van beheersing van de door de leverancier uitbestede (deel) processen. Deze inzet, beheersing en wijziging van sub verwerking wordt opgenomen in de overeenkomst met de leverancier.
N. Periodiek overleg en rapportages; a)	ProRail ontvangt periodiek rapportages van de leveranciers over de geleverde prestatie met betrekking tot informatiebeveiliging en bespreekt die conform een vooraf afgesproken frequentie
N. Periodiek overleg en rapportages; b)	In het geval van af te nemen diensten met afgesproken serviceniveaus op gebied van informatiebeveiliging wordt tussen de leverancier en ProRail een SLA afgesloten.
O. Personeel; a)	Een recente Verklaring Omtrent het Gedrag (VOG) is vereist voor medewerkers van de leverancier die werkzaamheden uitvoeren op locaties van ProRail of die toegang krijgen tot apparatuur, infrastructuur of gegevens van ProRail. De noodzaak en wijze van aanlevering wordt vooraf afgestemd met ProRail.
O. Personeel; b)	ProRail kan het personeel van de leverancier, dat voor de uitvoering van het contract wordt ingeschakeld, aan een veiligheidsonderzoek (laten) onderwerpen als bijvoorbeeld een Vertrouwensfunctie wordt vervuld. De leverancier verleent aan dat onderzoek zijn volledige medewerking. ProRail kan op grond van de uitkomsten daarvan de inzet van het betrokken personeelslid bij de uitvoering van de overeenkomst weigeren
O. Personeel; c)	Indien een medewerker van de leverancier, die door zijn werkzaamheden op locatie van ProRail komt en/of toegang heeft tot infrastructuren en gegevens, uit dienst gaat, wordt dit minimaal twee weken van tevoren gemeld aan de contractmanager van ProRail.
P. Retour/vernietiging bedrijfsmiddelen en informatie; a)	Op verzoek retourneert of vernietigt de leverancier, dit naar keuze van ProRail, onverwijld alle door ProRail ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevensdragers en back-ups). Dit geldt ook voor alle gegevens, inclusief persoonsgegevens, ook in cloudomgevingen.
P. Retour/vernietiging bedrijfsmiddelen en informatie; b)	Voorafgaand aan hergebruik of verwijdering van apparatuur dienen alle gegevens op de daarin aanwezige opslagmedia op betrouwbare wijze te worden verwijderd. Dit gebeurt door een hiertoe gecertificeerde organisatie. Als bewijs van verwijdering dient een certificaat door het vernietigingsbedrijf te worden aangeleverd.
Q. Auditrecht	ProRail kan op enig moment een audit, waaronder een penetratietest, (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit is niet nodig als de leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met ProRail.

R. Risicomanagement; a)	De gecontracteerde leverancier dient gedurende de looptijd van het contract te beschikken over een actuele, gedocumenteerde en door zijn management geaccordeerde classificatie en risicoanalyse, uitgevoerd voor de te leveren IT-en OT-diensten. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de continuïteit van de bedrijfsprocessen van ProRail zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald.
R. Risicomanagement; b)	Beheersmaatregelen die voortkomen uit de risicoanalyse en waar ProRail een aandeel in de implementatie heeft, worden afgestemd met ProRail.
R. Risicomanagement; c)	De leverancier dient ProRail (op verzoek) te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.
S. Security en BCM by Design	De gangbare principes rondom Security by Design/Default en BCM by Design zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet binnen de opdracht inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
T. Security testing; a)	ProRail kan een security test, zoals een penetratietest, laten uitvoeren als onderdeel van de acceptatie en/of validatie om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Een security test is niet nodig als de leverancier door middel van rapportages aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke security test heeft plaatsgevonden en de relevante resultaten deelt met ProRail.
T. Security testing; b)	Indien ProRail in het kader van acceptatie of validatie een security test (laat) verricht(en), stelt ProRail zo spoedig mogelijk een testverslag op en zendt dat ondertekend aan Opdrachtnemer. In het testverslag worden geconstateerde bevindingen en gebreken vastgelegd alsook of ProRail de geteste asset goed- of afkeurt. Afspraken worden tussen ProRail en de leverancier gemaakt over de opvolging van de bevindingen.
U. Toegang tot digitale infrastructuur en gegevens; a)	Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT- en OT-systemen van ProRail. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.
U. Toegang tot digitale infrastructuur en gegevens; b)	De toegang van medewerkers van de leverancier tot ProRail informatie en systemen is beperkt tot datgene dat nodig is voor het leveren van de dienst (need to know principe).
U. Toegang tot digitale infrastructuur en gegevens; c)	Alleen bij een aantoonbare noodzaak krijgen leveranciers remote toegang tot de ProRail omgeving.
U. Toegang tot digitale infrastructuur en gegevens; d)	Remote toegang tot en beheer op afstand van IT- en OT-omgevingen, uitgevoerd door de leverancier, dienen te worden gemonitord.
V. Toegang tot fysieke infrastructuur	Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen, wat geborgd is in een (mechanisch) sluitplan.
W. Wijzigingsbeheer	Substantiële wijzigingen van de leveranciersorganisatie en -processen met impact voor ProRail dienen door de leverancier tijdig kenbaar gemaakt te worden aan ProRail. Dit wordt opgenomen als onderdeel van de overeenkomst met de leverancier.